FORMOSA
Wireless Systems Corp.

IEEE 802.11 Series
NLOS Outdoor Wireless AP
KW9000 NLOS BRIDGE

User's Manual

V 4.8.7.0

Formosa Wireless Systems Corp.
http://www.tw-wireless.com

DARK Group 大可集團

1. Copyright

There is no any clear or implicit assurance in the user's manual of our company, including the assurance of selling or installing for the special purpose. There are rival's volumes to carry on the power to alter or revise in our company, if alter and forgive me for not issuing a separate notice. You can’t duplicate any content of this manual by the written permission of our company.

2. About the manual

The purpose to use this manual is for install the wireless Access Point. This manual is including disposing course and method and helping the customer to solve the unpredictable problem.

The following typographical conventions are used in this purpose:

✎ **Notice:**

- This indicates an important Note.

⚠ **Warning**

- This indicates a warning or caution.

Bold: Indicates the function, important words, and so on.

Content

Content of Figure

Chapter 1 Introduction

Introduction

Thank you for choosing the Formosa's KWO9000 Access Point (hereafter called access point). This Access Point provides a secure, affordable, and easy-to-use wireless LAN solution that combines mobility and flexibility with the enterprise-class features required by networking professionals.

Appearance of Product

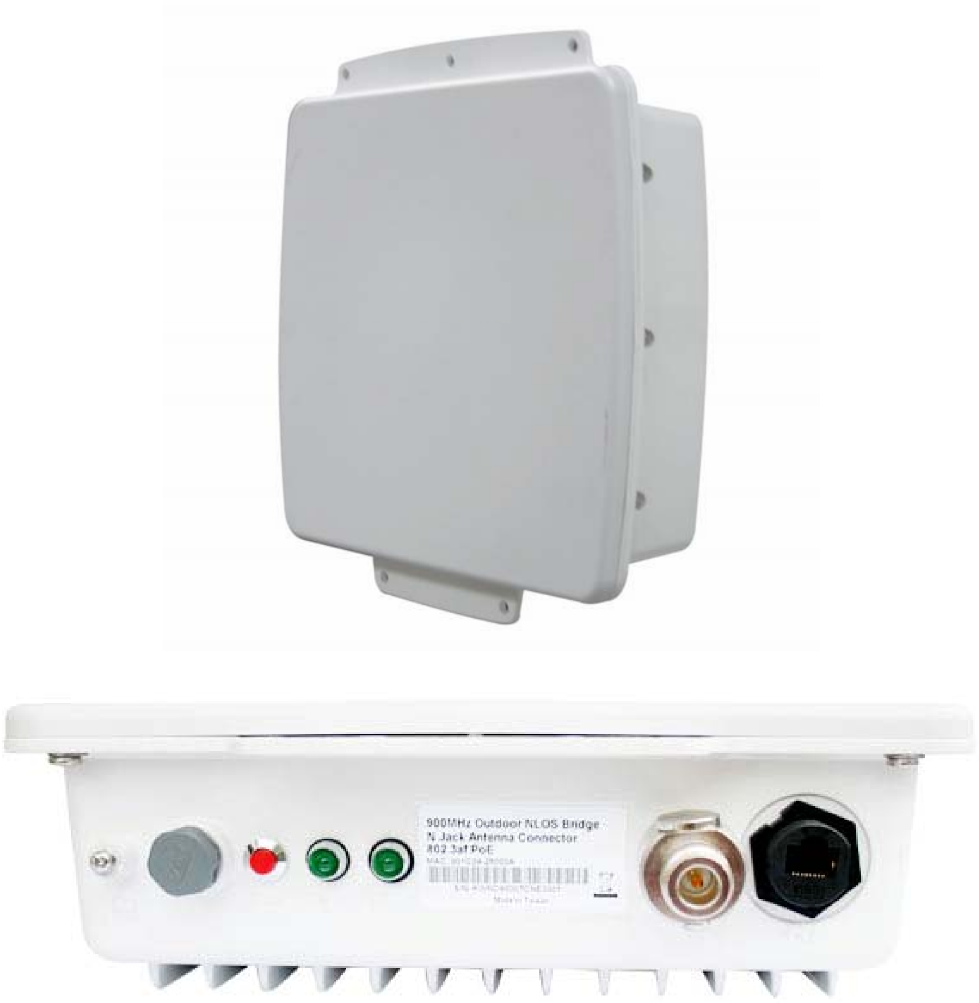


Figure 1 KW9000 NLOS Bridge

Features and Benefits

- Support power over Ethernet
- IP67 class of enclosure
- Wireless module works as 5GHz
- Easy to install and friendly to user, just plug and play
- MAC address control
- Provides Web-based configuration utility
- Tight design with lightweight, compact size, and low power consumption
- All wireless nodes auto-discover and self-configure
- Provide the highest available level of WEP/WPA PSK security
- NLOS (non-line-of-sight)
- Support the function of QoS (WMM) / Multi-BSSID/VLAN

Chapter 2 Hardware Installation

System Requirement

- Two PCs with RJ-45 connector NIC supporting the transfer rate of 10/100Mbps data.
- The IP address of NIC should be the same subnet with the AP, the default IP address of AP is 192.168.1.1.
- Microsoft Internet Explorer 6 updated with Service Pack 1 or the newer patch Q323308.

Product Kit

- KW9000 NLOS BRIDGE×1
- Injector-N (48V, 1A)×1
- Accessories×1
- Product CD×1

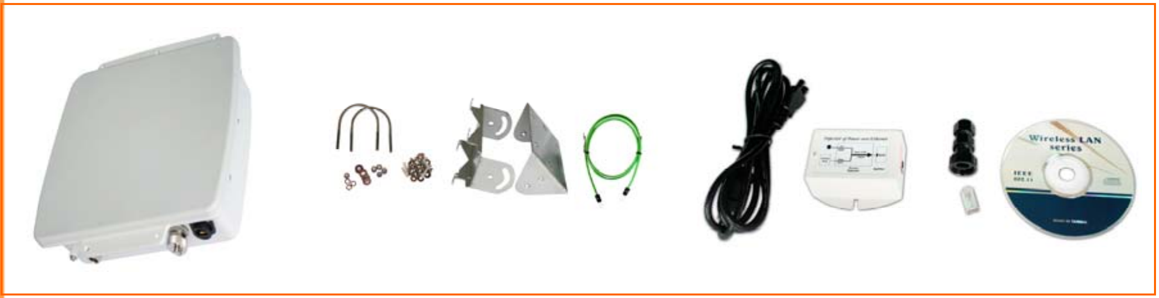
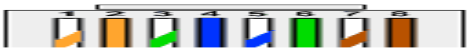


Figure 2 device

Hardware Installation

Take the following steps to set up the device.

1. All the parts of product are shown as following picture.
2. Put an Ethernet cable with RJ-45 connector through the water-joint. If there no such cable, Make the RJ-45 connector as the following rules:



3. Attach Ethernet cable to the RJ-45 connector on the Access Point. Then connect another end of the RJ-45 cable to a hub or a terminal.
4. Plug water-joint into the Access Point and tighten it.
5. Connect the Access Point to the ground via ground connection which is beside the RJ-45 port.
6. Attach the external antenna to Access Point.
7. Thus all, the hardware installation is completed.

Antenna Installation

Install two Antennas to the equipment.

⚠ **Warning**

- Please do not put Access Point near these places: electric power line, electric light, electricity or any places nearby strong electric power, otherwise it may make damage to Access Point.

Chapter 3　System Setup

Default Setting

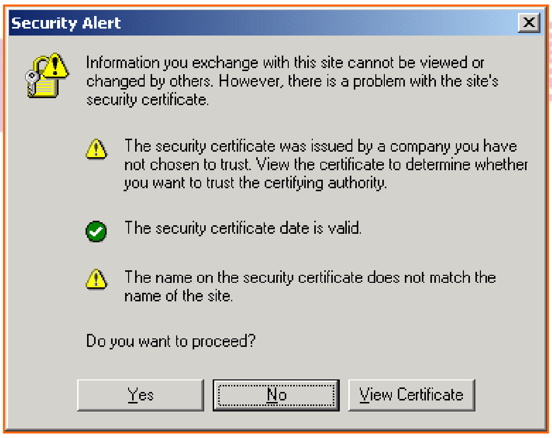
Diagram 1 Default Settings

Options	Default Value
User Name	admin
Password	password
Wireless Device Name	DEVICExxxxxx（xxxxxx indicate the last 6 MAC address of Wireless B）
Ethernet Data Rate	Automatic
IP Address	IP Address : 192.168.1.1 Mask : 255.255.255.0 Gateway: 0.0.0.0 Primary DNS Server: 0.0.0.0 Secondary DNS Server: 0.0.0.0
Data Rate	Best
Output Power	Full
RTS Threshold	2346
Fragmentation Threshold	2346
Wireless Space	10000
Enable Refuse XDos	No
Security Settings	Disable
Default Channel	52/5.260GHz or 1/2.412GHz
Band Width	5MHz
Spanning Tree Protocol	Enable
SNMP Settings	SNMP：Enable Read Community：public Write Community：private

Using the Web Management

The Web Management provides you with a user-friendly graphical user interface. The Access Point allows you via web browser (MS Internet Explorer 6.0) to monitor and configure the device.

1. Run Web Explorer, Enter default IP Address: **http://192.168.1.1** in the Address field. After press Enter key then pop up a security alarm page, the page will show up:



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

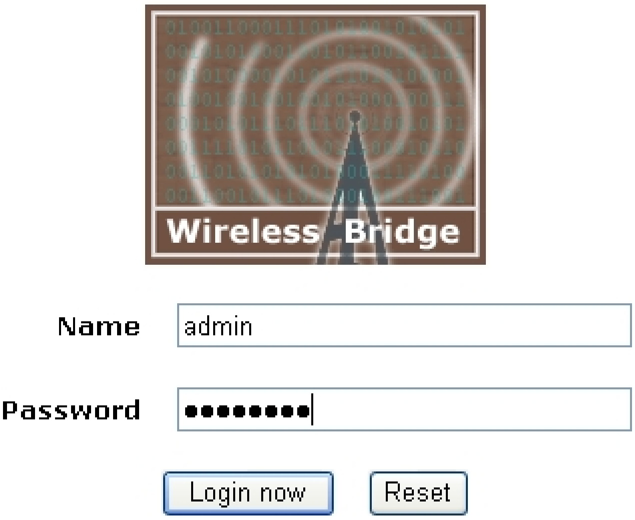
✓ The security certificate date is valid.

⚠ The name on the security certificate does not match the name of the site.

Do you want to proceed?

Figure 3 Security Alarm

2. Click yes button, the login page will show up.

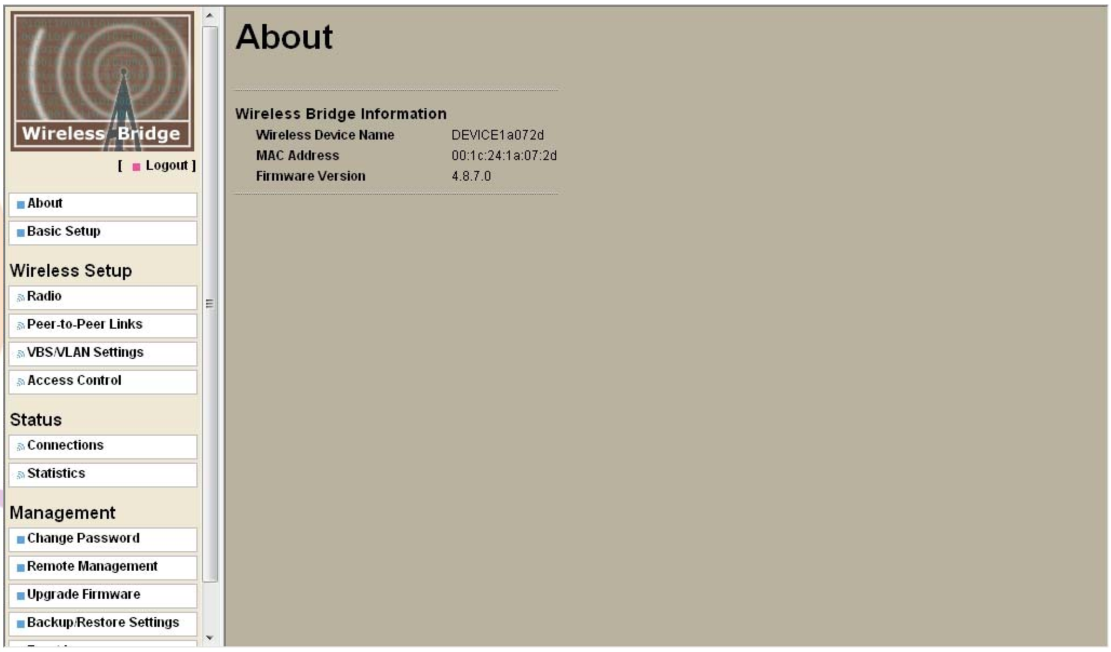


Name admin

Password ●●●●●●●●●

Figure 4 Login

3. Enter default User Name (admin) and default Password (password), Click Login. The home page will show up.



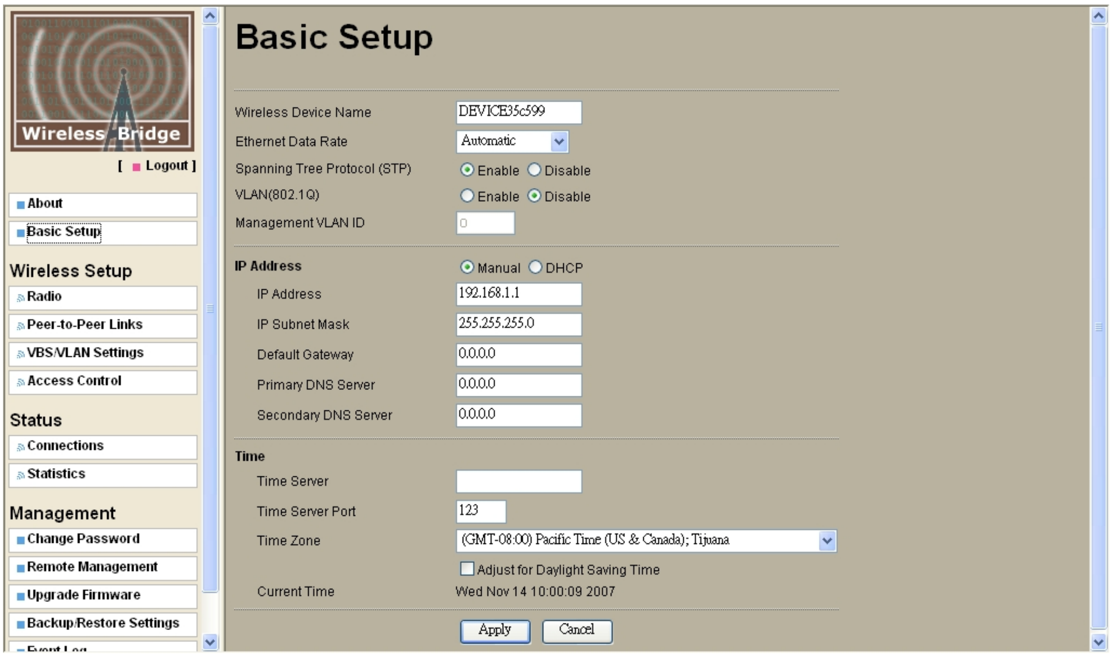
About

Wireless Bridge Information

Wireless Device Name	DEVICE1a072d
MAC Address	00:1c:24:1a:07:2d
Firmware Version	4.8.7.0

Figure 5 Information Page

Set the Basic Configuration



Basic Setup

Wireless Device Name	DEVICE35c599
Ethernet Data Rate	Automatic
Spanning Tree Protocol (STP)	● Enable ○ Disable
VLAN(802.1Q)	○ Enable ● Disable
Management VLAN ID	0
IP Address	● Manual ○ DHCP
IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Time	
Time Server	
Time Server Port	123
Time Zone	(GMT-08:00) Pacific Time (US & Canada); Tijuana
	□ Adjust for Daylight Saving Time
Current Time	Wed Nov 14 10:00:09 2007

Figure 6 Basic setup

Wireless Device Name

This is the NetBIOS name of Access Point; you may modify the default name with a unique name up to 15 characters long including numbers from 0 to 9, letters (A-Z; a-z) and digraphs

(-), the name supports WINS so you can ping Access Point using "ping Access Point Name" or use web browser to open web utility by inputting Access Point Name in the IE address.

Notice:

- The default Access Point Name is: DEVICExxxxxx (xxxxxx represents the last 6 digits of MAC address.
- The first character of Access Point Name cannot be digits.
- Your host must have a TCP/IP address with the same subnet as the Access Point while using WINS.

- **Ethernet Data Rate：**

  Specify the ethernet port's data rate.
- **Spanning Tree Protocol(STP):**

  Enabling spanning tree can prevent undesirable loops in the network, ensuring a smooth running network. By default, the function is enabled.
- **Time Server Port**

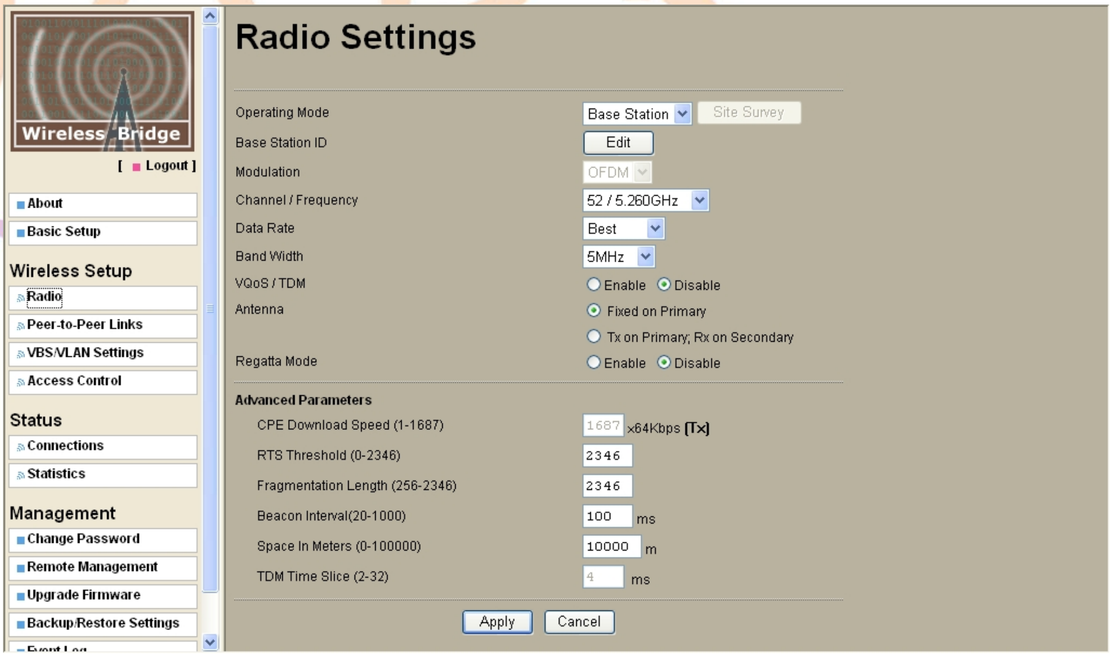
  This field identifies the time server port like 123.
- **Time Zone**

  Select the time zone location for your setting.
- **Current Time**

  This field identifies the current time in your specific time Zone.

Chapter 4 Wireless Setup

Radio



Radio Settings

Operating Mode: Base Station | Site Survey

Base Station ID: Edit

Modulation: OFDM

Channel / Frequency: 52 / 5.260GHz

Data Rate: Best

Band Width: 5MHz

VQoS / TDM: ○ Enable ● Disable

Antenna: ● Fixed on Primary ○ Tx on Primary; Rx on Secondary

Regatta Mode: ○ Enable ● Disable

Advanced Parameters

CPE Download Speed (1-1687): 1687 x64Kbps [Tx]

RTS Threshold (0-2346): 2346

Fragmentation Length (256-2346): 2346

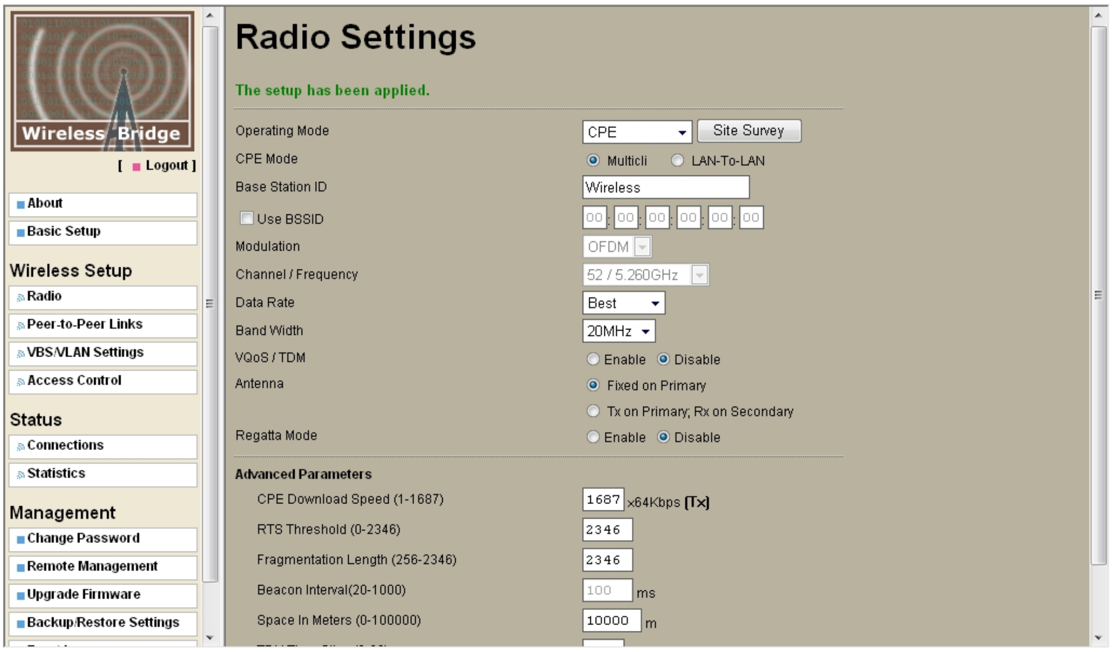
Beacon Interval(20-1000): 100 ms

Space In Meters (0-100000): 10000 m

TDM Time Slice (2-32): 4 ms

Apply | Cancel

Figure 7 Base Station Mode



Radio Settings

The setup has been applied.

Operating Mode: CPE | Site Survey

CPE Mode: ● Multicli ○ LAN-To-LAN

Base Station ID: Wireless

□ Use BSSID: 00 : 00 : 00 : 00 : 00 : 00

Modulation: OFDM

Channel / Frequency: 52 / 5.260GHz

Data Rate: Best

Band Width: 20MHz

VQoS / TDM: ○ Enable ● Disable

Antenna: ● Fixed on Primary ○ Tx on Primary; Rx on Secondary

Regatta Mode: ○ Enable ● Disable

Advanced Parameters

CPE Download Speed (1-1687): 1687 x64Kbps [Tx]

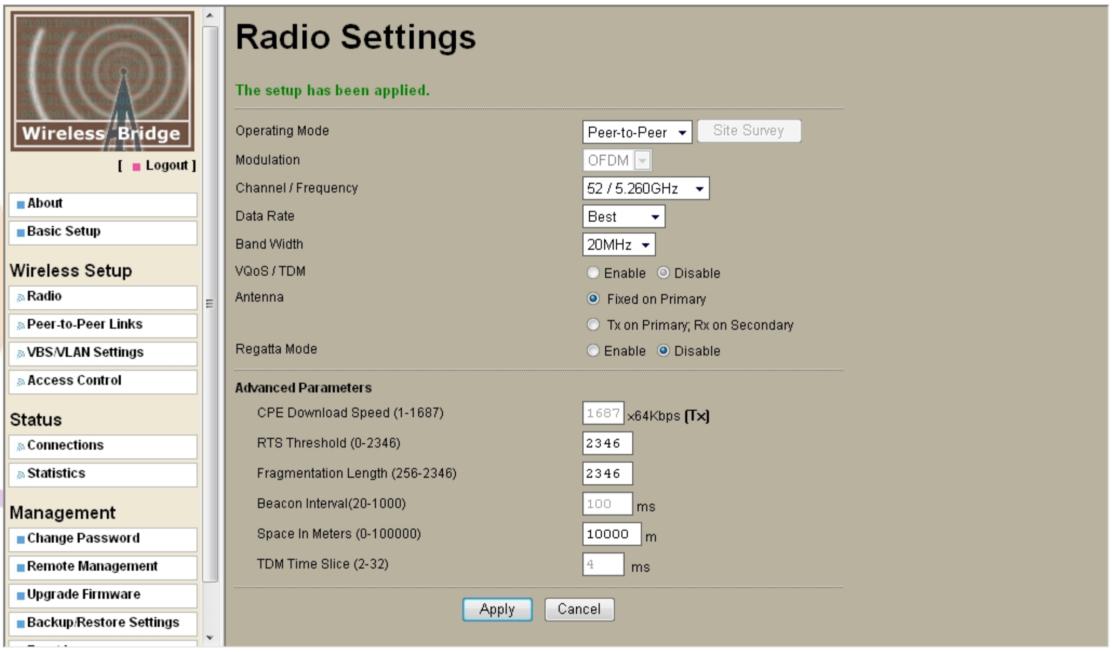
RTS Threshold (0-2346): 2346

Fragmentation Length (256-2346): 2346

Beacon Interval(20-1000): 100 ms

Space In Meters (0-100000): 10000 m

Figure 8 CPE Mode



Radio Settings

The setup has been applied.

Operating Mode	Peer-to-Peer
Modulation	OFDM
Channel / Frequency	52 / 5.260GHz
Data Rate	Best
Band Width	20MHz
VQoS / TDM	○ Enable ● Disable
Antenna	● Fixed on Primary ○ Tx on Primary; Rx on Secondary
Regatta Mode	○ Enable ● Disable

Advanced Parameters

CPE Download Speed (1-1687)	1687 x64Kbps [Tx]
RTS Threshold (0-2346)	2346
Fragmentation Length (256-2346)	2346
Beacon Interval(20-1000)	100 ms
Space In Meters (0-100000)	10000 m
TDM Time Slice (2-32)	4 ms

Figure 9 Peer-to-Peer Mode

- **Operating Mode:**

Select the operating mode as NLOS Network Enable the NLOS function.

Base Station : Act as a standard 802.11a/b/g. The default mode is Base Station..

CPE：Perform as a client station associated to other APs. Be sure that they share the same SSID when connected.

Peer-to-Peer：Select this only if this KWO9000 is the “Master” for a group of bridges. The other bridge must use this KWO9000 MAC address. They then send all traffic to this “Master”, rather than communicate directly with each other. WEP should be used to protect this traffic.

- **Wireless Network Name (SSID)**

The SSID is a unique ID used by Access Points and Stations to identify a wireless LAN. Wireless clients associating to any Access Point must have the same SSID. The default ESSID is “**Wireless**”. The ESSID can up to 32 characters

- **Broadcast Wireless Network Name (SSID)**

If you hide the SSID, then the device cannot be seen when a wireless client scans for local APs. The trade-off for the extra security of “hiding” the device may be inconvenience for some valid WLAN clients.

- **Default Channel:**

Select the channel that you plan to use.

- **Diagram 3 Channel/Frequency List（2.4GHz）**

Channel	Frequency
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462

- **Diagram 4 Channel/Frequency List（5GHz）**

Channel	Frequency
52	5260
53	5265
54	5270
55	5275
56	5280
57	5285
58	5290
59	5295
60	5300
61	5305
62	5310
62	5315
64	5320
149	5745
150	5750
151	5755
152	5760
153	5765

154	5770
155	5775
156	5780
157	5785
158	5790
159	5795
160	5800
161	5805
162	5810
163	5815
164	5820
165	5825

- **Antenna**

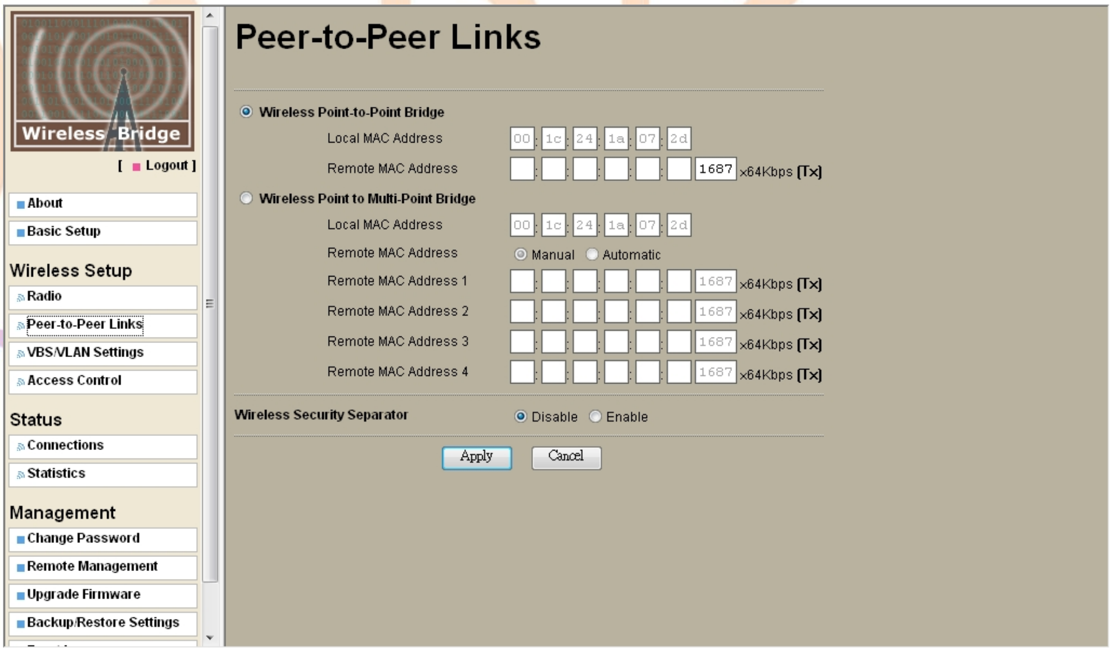
Select the desired antenna for transmitting and receiving. Auto is the default.

- **Diagram 5 wireless lan parameters**

Field	Description
RTS Threshold	The packet size used to determine whether it should use the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) or the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) mechanism for packet transmission.
Fragmentation Length	This is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold
Beacon Interval	Specifies the data beacon rate between 20 and 1000.

Peer-to-Peer Links

In Peer-to-Peer mode, you can set Point-to-Point Bridge and Point to Multi Point here.



Peer-to-Peer Links

● Wireless Point-to-Point Bridge

Local MAC Address 00 : 1c : 24 : 1a : 07 : 2d

Remote MAC Address _ : _ : _ : _ : _ : _ 1687 x64Kbps [Tx]

○ Wireless Point to Multi-Point Bridge

Local MAC Address 00 : 1c : 24 : 1a : 07 : 2d

Remote MAC Address ● Manual ○ Automatic

Remote MAC Address 1 _ : _ : _ : _ : _ : _ 1687 x64Kbps [Tx]

Remote MAC Address 2 _ : _ : _ : _ : _ : _ 1687 x64Kbps [Tx]

Remote MAC Address 3 _ : _ : _ : _ : _ : _ 1687 x64Kbps [Tx]

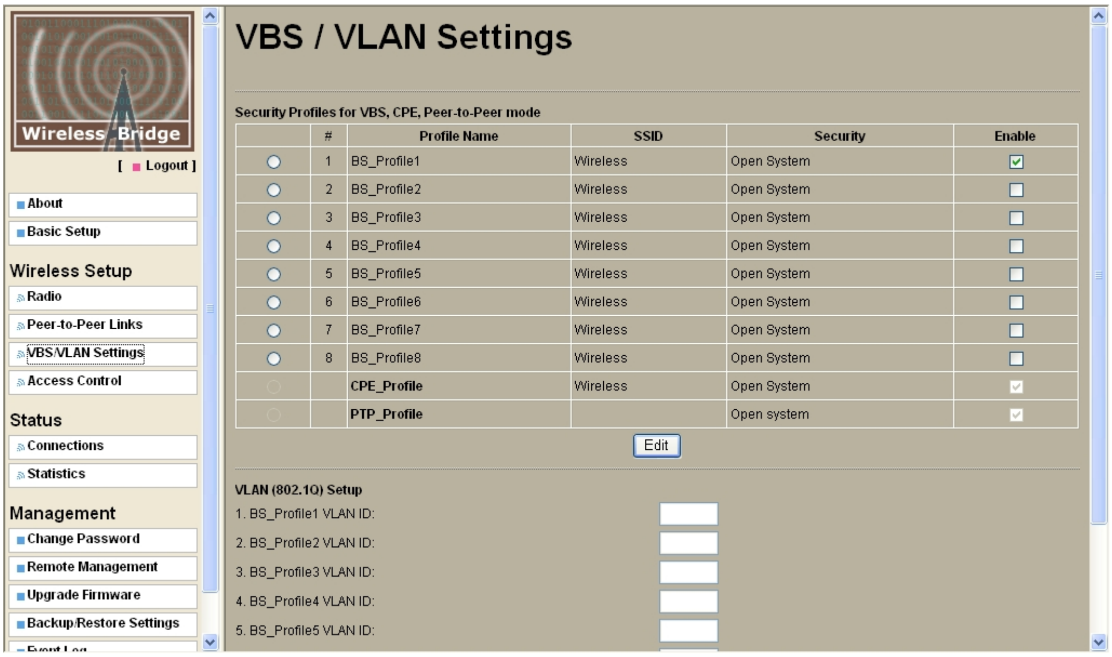
Remote MAC Address 4 _ : _ : _ : _ : _ : _ 1687 x64Kbps [Tx]

Wireless Security Separator ● Disable ○ Enable

Figure 10 Peer-to-Peer Links

VBS/VLAN Settings

In Base Station mode, you could enable 802.1Q VLAN to manage users, **You could select one profile to edit as follow:**



VBS / VLAN Settings

Security Profiles for VBS, CPE, Peer-to-Peer mode

	#	Profile Name	SSID	Security	Enable
○	1	BS_Profile1	Wireless	Open System	☑
○	2	BS_Profile2	Wireless	Open System	□
○	3	BS_Profile3	Wireless	Open System	□
○	4	BS_Profile4	Wireless	Open System	□
○	5	BS_Profile5	Wireless	Open System	□
○	6	BS_Profile6	Wireless	Open System	□
○	7	BS_Profile7	Wireless	Open System	□
○	8	BS_Profile8	Wireless	Open System	□
○		CPE_Profile	Wireless	Open System	☑
○		PTP_Profile		Open system	☑

VLAN (802.1Q) Setup

1. BS_Profile1 VLAN ID: ___

2. BS_Profile2 VLAN ID: ___

3. BS_Profile3 VLAN ID: ___

4. BS_Profile4 VLAN ID: ___

5. BS_Profile5 VLAN ID: ___

Figure 11 VBS/VLAN Settings

One device could be used to eight devices. So you could easy setup your network and manage different users. And the eight VBS could set different security to protect your network.

- **Management VLAN ID**

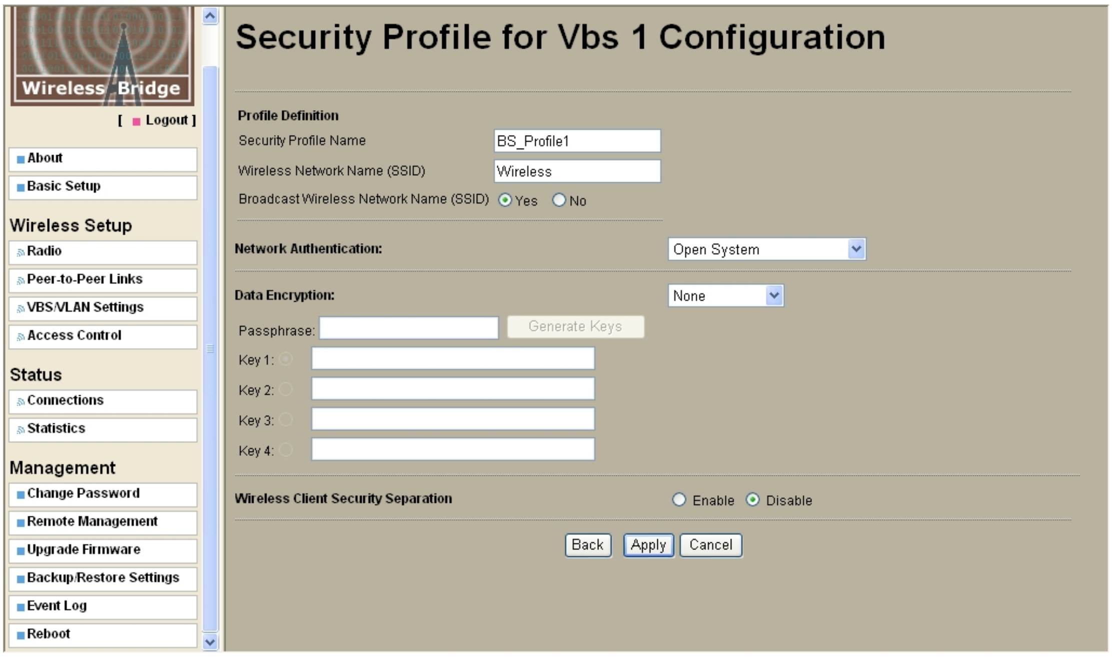
  Management VLAN ID is used to manage device and monitor the network.

- **Security Profile VLAN ID**

  Security Profile VLAN ID is used to manage VLAN. You could set ID 1~4049.

Security Profile Settings following steps below:

Security Profile



Security Profile for Vbs 1 Configuration

Profile Definition

Security Profile Name: BS_Profile1

Wireless Network Name (SSID): Wireless

Broadcast Wireless Network Name (SSID) ● Yes ○ No

Network Authentication: Open System

Data Encryption: None

Passphrase:

Key 1: ○

Key 2: ○

Key 3: ○

Key 4: ○

Wireless Client Security Separation ○ Enable ● Disable

Figure 12 Security Profile

- **Authentication Type**

  Choose the following type.

  - Open System: Allow any wireless NIC or wireless bridge connect
  - Shared Key: If Shared Key is selected, you need to enabled WEP and enter at least one shared key.

- 802.1x: IEEE 802.1x is a standard for network access control (port based), which was introduced especially for distributing encryption keys in a wireless network. The Access Point supports 802.1x for keeping out unauthorized users and for verifying the credentials of users with RADIUS so that authorized users can access the network and services. To use 802.1x, you will need at least one common Extensible Authentication Protocol (EAP) method on your authentication server, Access Points (authenticator) and stations (supplicant). 802.1x is also used to perform generation and distribution of encryption keys with enabling Data Encryption as WEP from AP to the station as part of or after the authentication process.
- WPA with Radius, WPA2 with Radius, WPA & WPA2 with Radius: In cooperation with RADIUS, systems with WPA-EAP will be used with a new encryption method called Temporal Key Integrity Protocol (TKIP) implementation with 802.1x dynamic key exchange.
- WPA-PSK, WPA2-PSK, WPA-PSK & WPA2-PSK: Instead of using RADIUS for authentication, systems with WPA-PSK will be configured with a secret password phrase. Enter your password phrase and press “Generate”. You can now create a pre-shared key in the Access Point and copy the characters you input to the station's WPA-PSK entry. A shared secret is only secure as long as no third party knows about it.

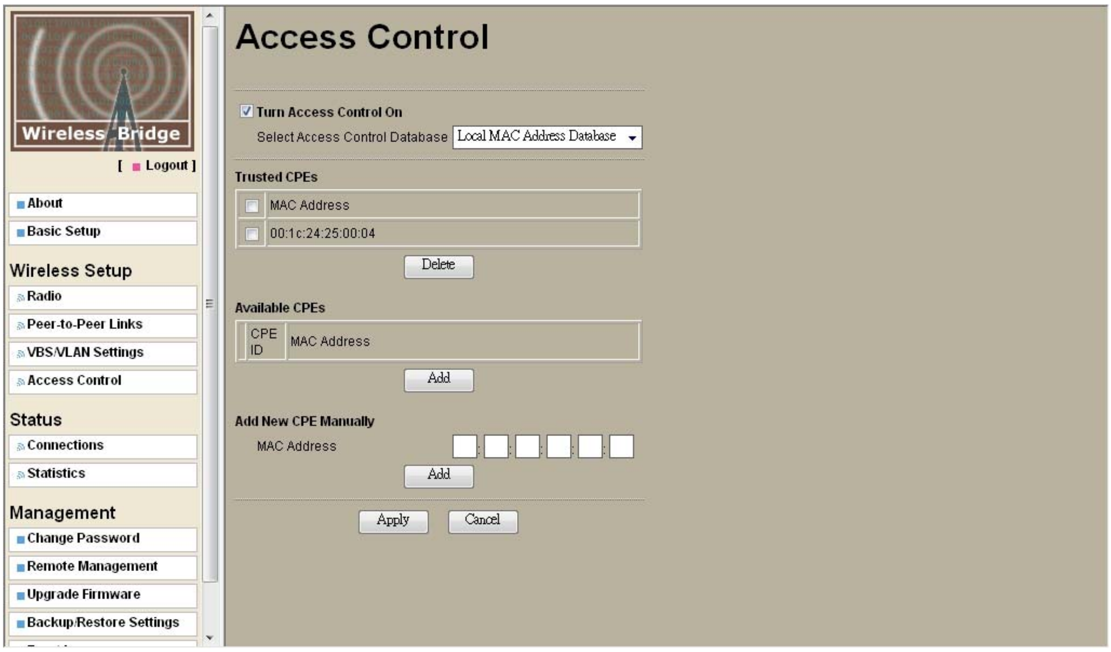
- **Diagram 6 The following elaborate WEP/WPA security options.**

Field	Description
Network Authentication	You have two authentication options. • Open System: No authentication is imposed to the KWO9000. However, if the 802.1x option is configured, authentication of connections can be performed by a RADIUS server. • Shared: this is for shared key authentication. Data is encrypted.
Encryption Strength	You can select the following data encryption options: Disabled 64- 128- or 152-bit WEP With Open System Authentication and 64- 128- or 152-bit WEP Data Encryption with Shared Key authentication
Security Encryption (WEP) Keys	WEP enabled, you can manually enter the four data encryption keys or enable Passphrase to generate the keys automatically. These values must be matched between all Clients and access points at your LAN (key 1 must be the same for all, key 2 must be the same for all, etc.) Two ways to create WEP encryption keys: • Passphrase. Passphrase functions as automatically case-sensitive characters. However not all wireless adapters support passphrase key generation. • Manual. These values are not case sensitive. 64-bit WEP: enter 10 hexadecimal digits (any combination of 0-9, a-f, or

	A-F). 128-bit WEP: enter 26 hexadecimal digits (any combination of 0-9, a-f, or A-F). 152-bit WEP: enter 32 hexadecimal digits (any combination of 0-9, a-f, or A-F).
WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)	WPA Pre-Shared-Key uses a pre-shared key to perform the authentication and generate the initial data encryption keys. Then, it dynamically varies the encryption key. It uses Temporal Key Integrity Protocol (TKIP) for encryption keys. However not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA.
WPA 2-PSK	Identical to WPA-PSK with the exception of the way to encryption keys. WPA2-PSK uses Advanced Encryption Standard(AES) for encryption keys.
WPA-PSK& WPA 2-PSK	You may have the option of WPA-PSK associated with TKIP. Alternatively, you can select WPA2-PSK associated with AES.

Access Control

The optional Access Control window lets you block the network access privilege of the specified stations through the Access Point. This provides an additional layer of security. There are two kinds of ACL.



Access Control

☑ Turn Access Control On

Select Access Control Database: Local MAC Address Database

Trusted CPEs

□	MAC Address
□	00:1c:24:25:00:04

Available CPEs

CPE ID	MAC Address

Add New CPE Manually

MAC Address □:□:□:□:□:□

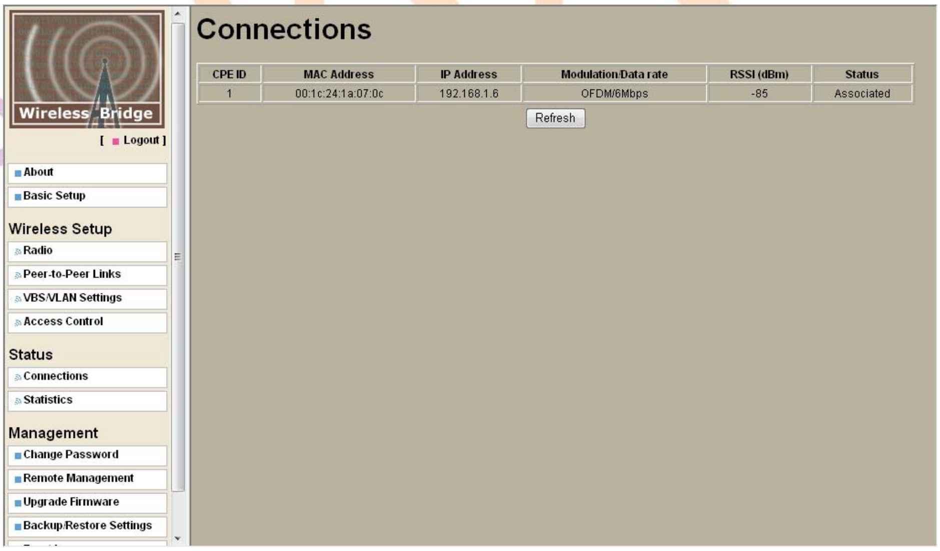
Figure 13 Access control

In Local MAC Address Database, you could enable Turn Access Control On and click Apply button. Only stations in the Trust list can connect AP and stations in Reject list can’t connect AP. What you should do is to maintenance the Available Wireless Stations list. While you set Radius parameters, you could use RADIUS MAC Address Database to control stations connection.

Chapter 5 Status

Connections

This page displays both wired Ethernet and wireless interface network traffic. Click Refresh to update the current statistics.



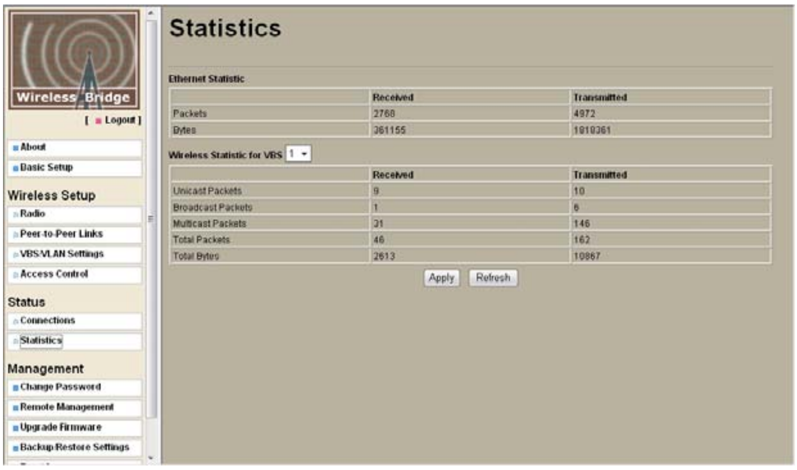
Connections

CPE ID	MAC Address	IP Address	Modulation/Data rate	RSSI (dBm)	Status
1	00:1c:24:1a:07:0c	192.168.1.6	OFDM/6Mbps	-85	Associated

Figure 14 Connections

Statistics

From the“Statistics” ，the KWO9000 provides information about sending or receiving packets out of both the Ethernet and wireless ports. Clicking “Refresh” allows you to view the real-time information linked to the KWO9000. All is read-only.



Statistics

Ethernet Statistic

	Received	Transmitted
Packets	2768	4972
Bytes	361155	1810361

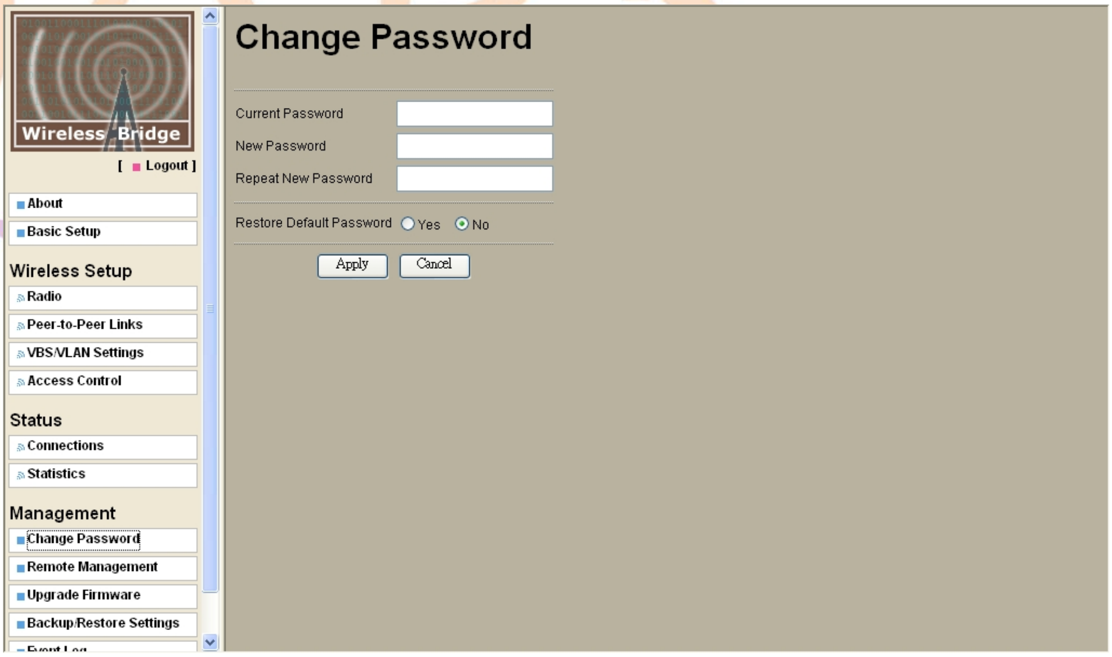
Wireless Statistic for VBS 1

	Received	Transmitted
Unicast Packets	9	10
Broadcast Packets	1	6
Multicast Packets	31	146
Total Packets	46	162
Total Bytes	2613	10867

Figure 15 Statistics

Chapter 6 Management

Change Password



Change Password

Current Password

New Password

Repeat New Password

Restore Default Password ○ Yes ● No

Figure 16 Change Password

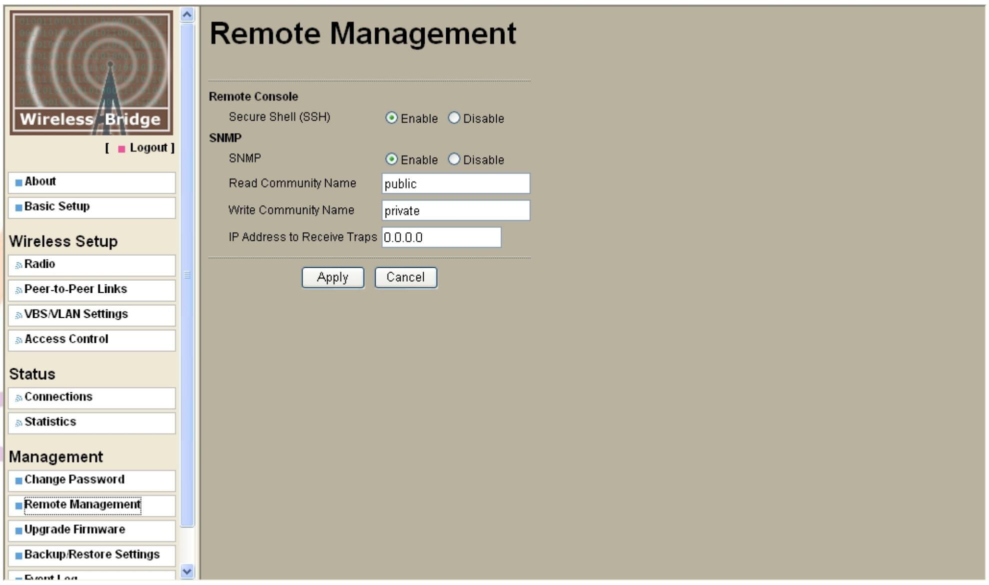
You can use the Change Password page to change the Access Point administrator's password for accessing the Settings pages.

To change the password, Type the old password. The default password for the Access Point is: password. Type a new password and type it again in the Repeat New Password box to confirm it.

Click Apply to have the password changed or click Cancel to keep the current password.

Be sure to write it down in a secure location and the maximal length of the password is 19 characters.

Remote Management



Remote Management

Remote Console

Secure Shell (SSH) ● Enable ○ Disable

SNMP

SNMP ● Enable ○ Disable

Read Community Name: public

Write Community Name: private

IP Address to Receive Traps: 0.0.0.0

Figure 17 Remote management

AP supports SNMP. At first you should set SNMP settings and get MIB file from AP by ftp.

SNMP Settings.

a) Set the Trap Server Address:

You can find the unusual log on the Trap Server.

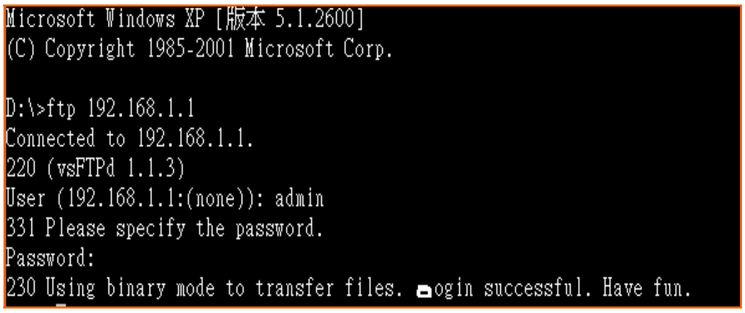
b) Set the Read-only Community;

c) Set the Read-write Community;

d) Click the “Apply” button to save setting.

1. Get MIB file by ftp

- Login AP by ftp.
- Input command “get pluto.mib”, you will find the MIB file in the current directory.



```
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 (vsFTPd 1.1.3)
User (192.168.1.1:(none)): admin
331 Please specify the password.
Password:
230 Using binary mode to transfer files. Login successful. Have fun.
```

Figure 18 get mib

Upgrade Firmware

There are two kinds way to upgrade Access Point software.

By WEB

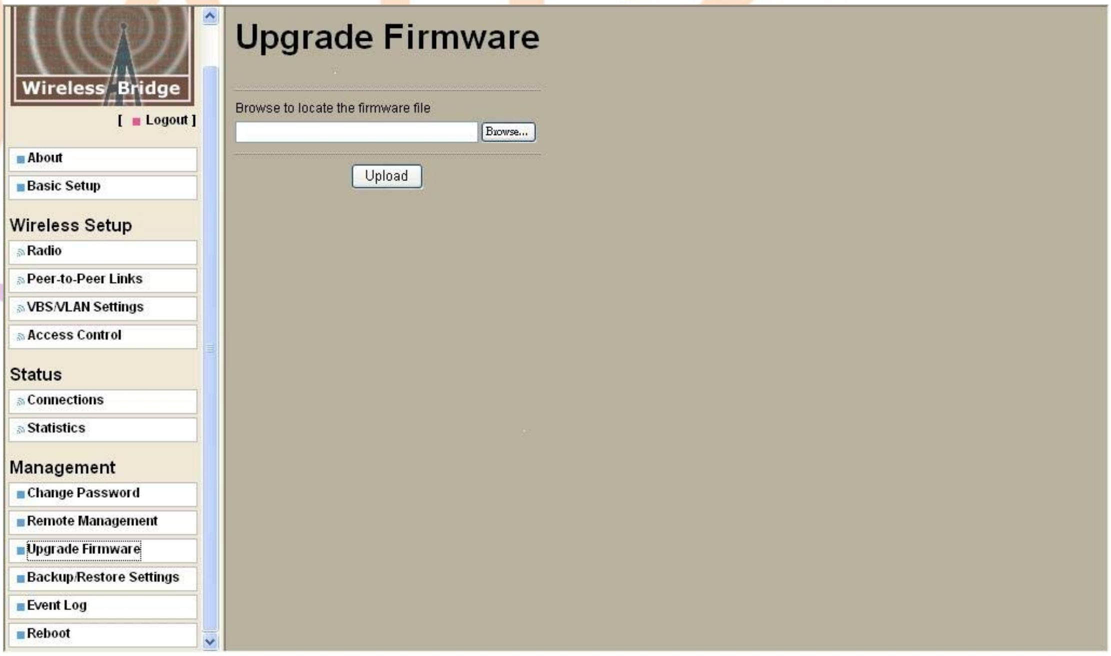


Figure 19 Upgrade firmware

1. Open Upgrade Firmware page

2. Click browser button and select the firmware file in local hard disk.

3. Click Upload button.

4. After upgrade, login again and check the software version.

By FTP

e) FTP 192.168.1.1(the AP IP address), input user (admin) and password (password).

f) After login in, input command “put KW9000.rmt”. Then the upgrade is going on automatically.

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220   (vsFTPd 1.1.3)
User   (192.168.1.1:(none)): admin
331 Please specify the password.
Password:
230 Using binary mode to transfer files.
ftp> put kw9000.rmt
200 PORT command successful. Consider using PASV.
```

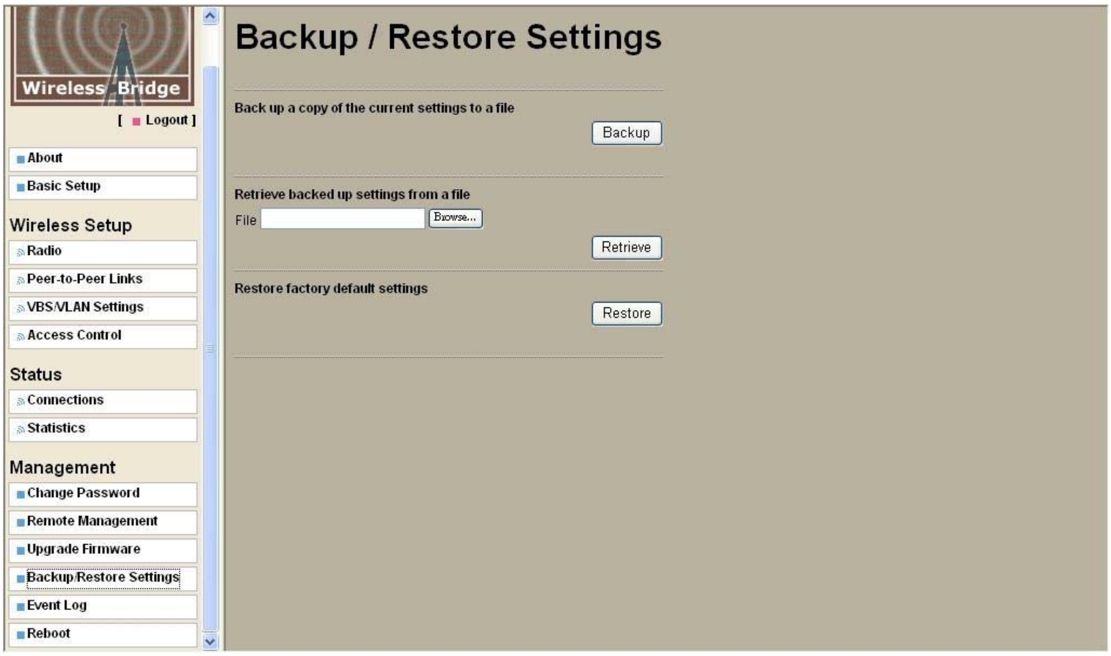
```
150 Ok to send data.
226 File receive OK.
ftp: 3973128 bytes sent in 0.55Seconds 7263.49Kbytes/sec.
ftp> quit
221 Goodbye.
```

Figure 20 upload firmware

Notice:

- The software must be KWA-O9000.rmt or kwa-o9000.rmt.
- Do not try to turn off the Access Point, shutdown the computer or do anything else to the Access Point until the Access Point finishes restarting!

Backup/Restore Settings



Backup / Restore Settings

Back up a copy of the current settings to a file

Retrieve backed up settings from a file

File

Restore factory default settings

Figure 21 Backup /Restore setting

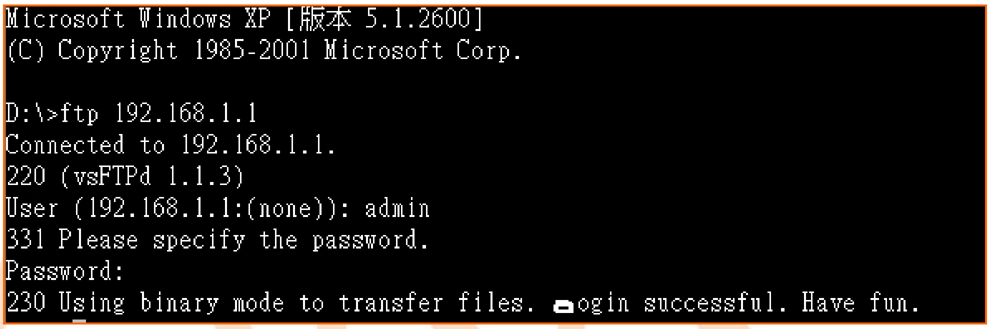
- **WEB**

1. Click button to save backup file to hard disk.
2. Click Browser button to locate the backup file you want to retrieve and click retrieve button, then the AP will restart.

- **FTP**

1. Login AP by ftp.

2. Input command get KW9000.cfg, it will be saved in current directory.



```
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 (vsFTPd 1.1.3)
User (192.168.1.1:(none)): admin
331 Please specify the password.
Password:
230 Using binary mode to transfer files. ▄ogin successful. Have fun.
```

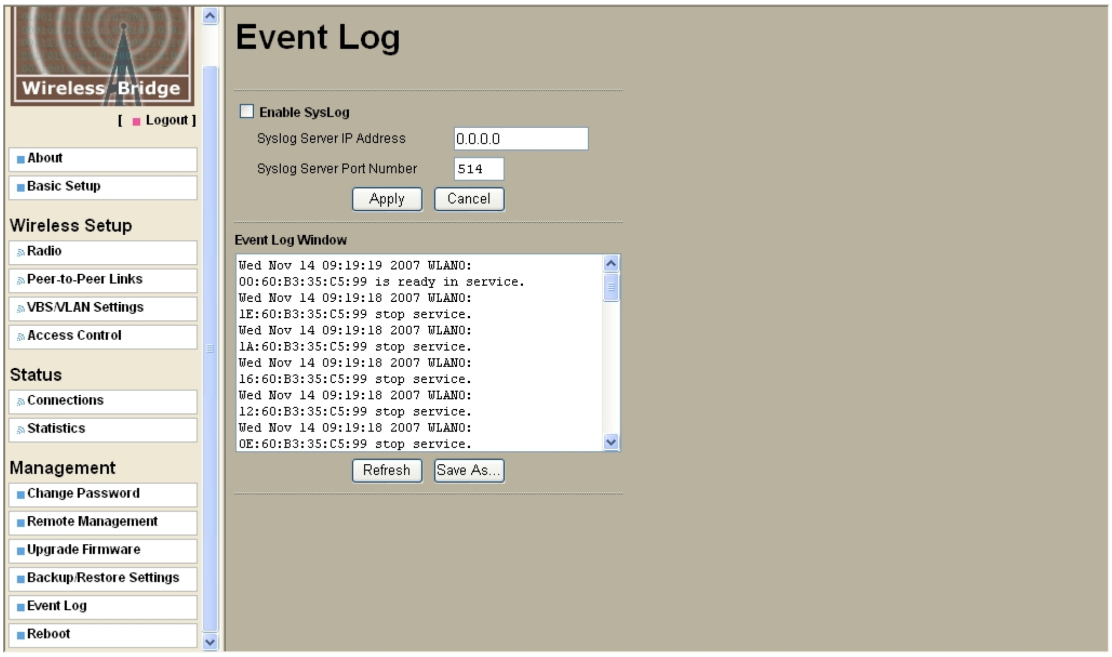
Figure 22 ftp get setting

3. Input command put KW9000.cfg, it will retrieve it to AP. and AP will restart.

Notice:

- The config file must be KW9000.cfg or kw9000.cfg
- Do not try to turn off the Access Point, shutdown the computer or do anything else to the Access Point until the Access Point finishes restarting!

Event Log



Event Log

□ Enable SysLog

Syslog Server IP Address: 0.0.0.0

Syslog Server Port Number: 514

Event Log Window

```
Wed Nov 14 09:19:19 2007 WLAN0:
00:60:B3:35:C5:99 is ready in service.
Wed Nov 14 09:19:18 2007 WLAN0:
1E:60:B3:35:C5:99 stop service.
Wed Nov 14 09:19:18 2007 WLAN0:
1A:60:B3:35:C5:99 stop service.
Wed Nov 14 09:19:18 2007 WLAN0:
16:60:B3:35:C5:99 stop service.
Wed Nov 14 09:19:18 2007 WLAN0:
12:60:B3:35:C5:99 stop service.
Wed Nov 14 09:19:18 2007 WLAN0:
0E:60:B3:35:C5:99 stop service.
```

Figure 23 Event log

If you have a SysLog server on your LAN, enable the SysLog option. Event Log offers you activity log information.

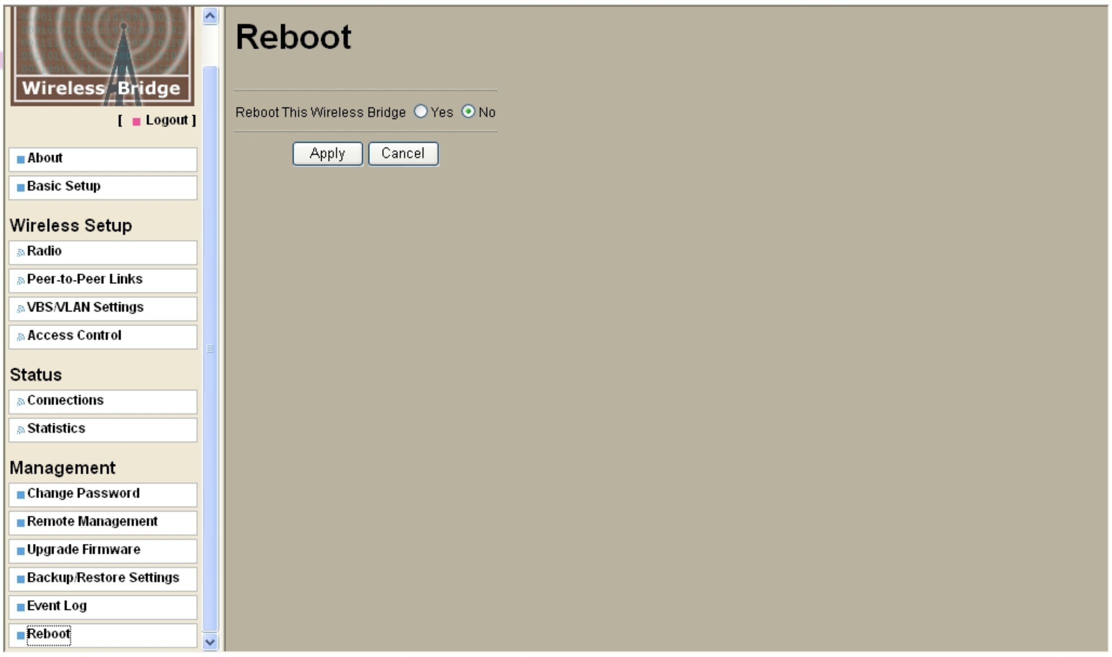
SysLog Server IP address

The access point will send all the SysLog to the specified IP address if SysLog option is enabled. Default: 0.0.0.0

Port

The port number configured in the SysLog server on your network. By default, it is514

Reboot AP



Reboot

Reboot This Wireless Bridge ○ Yes ● No

Figure 24 Reboot AP

You may select Yes on “Reboot AP” page and then click on APPLY button to reboot the access point.

Chapter 7 Troubleshooting

FAQ

Q 1. How to know the MAC address of the Access Point?

- The MAC address is written in a label which is in the bottom of Access Point.
- From the General page of WEB configuration, you also can get the MAC address of AP.

Q 2. Why the throughput is not high?

- You should adjust antenna to get highest signal strengthens. If can not get higher signal strengthens, please check the following steps:
- Wireless Channel/Frequency. Try to change other channel.
- Wireless disturbance. Check whether there are other wireless equipments nearby AP; make sure they do not disturb AP.
- To check if the antenna becomes flexible.
- To check signal strength. If the signal strength is very low, you may check the antenna or the device aging.
- To check the STA, and its output power may be low.

Q 3. Why two Access Points can not build connection after setting?

- Check the “Country/Region” whether is same.
- Check the “Channel/Frequency” whether is same.
- Check the “Data Encryption” and “Key” whether is same.

Q 4. The wireless becomes unstable such as ping timed out and lose packet after a period of well work?

- This situation may the wireless network is disturbed by something, what you can do is following steps:
- check whether every joint point of network is well（such as Ethernet port，antenna connection）
- Change the channel if the Link Test value is not high，excluding other wireless equipments disturb AP.
- Restart AP.
- Default AP and restore last settings.
- Check the wireless port and Ethernet port environment and virus exist or not.
- Please call the sales if can not solve problem after all.

Q 5. How to adjust output power?

- In the Wireless Settings page, you can do it.

Diagram 5 Output Power

	Full	1/2	1/4	1/8	Min
Output Power	15dbm	12dbm	9dbm	6dbm	3dbm

Q 6. Why can not open WEB page of remote wireless NLOS in local network?

- Because this kind of settings will slow the response of remote AP WEB Server, just waiting for several minutes or restarting remote wireless bridge is a way to solve problem. We suggest you set AP in local wired Ethernet network.

- Glossary

▪ **Diagram 7 Glossary**

Glossary	Expiation
802.11a	IEEE specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 5GHz. 802.11a provides specifications for wireless ATM systems and is used in access hubs. Networks using 802.11a operate at radio frequencies between 5.180 GHz and 5.825 GHz. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. In 802.11a, data speeds as high as 54 Mbps are possible.
802.11g	IEEE802.11g uses the 2.4 GHz frequency for greater range. 802.11g supports bandwidth up to 54 Mbps and is backwards compatible with 802.11b.
Access Point	In a wireless local area network (WLAN), an Access Point is a station that transmits and receives data (sometimes referred to as a transceiver). An Access Point connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network. Each Access Point can serve multiple users within a defined network area; as people move beyond the range of one Access Point, they are automatically handed over to the next one. A small WLAN may only require a single Access Point; the number required increases as a function of the number of network users and the physical size of the network.
WEP	Wired Equivalent Privacy is a data encryption protocol for 802.11 wireless networks. All wireless nodes and access points on the network are configured with a 64-bit, 128-bit or 152-bit Shared Key for data encryption.
Access Control	This function is only valid under AP mode, invalid under the mode of bridge graft. Used in MAC address to filter.
Bridge	Bridge is the device that connects and transmits data packets with two subnets

	by the same protocol and it works in the LLC layer of OSI.
DHCP 、 DHCP Client 、 DHCP Server	DHCP stands for "Dynamic Host Configuration Protocol". DHCP's purpose is to enable individual computers (DHCP Client) on an IP network to extract their configurations from a server (the 'DHCP server') or servers, in particular, servers that have no exact information about the individual computers until they request the information. The overall purpose of this is to reduce the work necessary to administer a large IP network. The most significant piece of information distributed in this manner is the IP address.
Encryption	For the security of transmit data in network, the data should be encrypted before transmit and decrypt received data.
IP Address	Internet Protocol is the main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.
LAN&WAN	LAN. A communications network serving users within a limited area, such as one floor of a building. A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.
MAC Address	Short for Media Access Control address, a hardware address that uniquely identifies each node of a network..
NetBIOS	Network Basic Input Output System. An application programming interface (API) for sharing services and information on local-area networks (LANs). Provides for communication between stations of a network where each station is given a name. These names are alphanumeric names, 16 characters in length.
Ping	A command line program in Windows, use it to check the connection whether is reachable.
Router	A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.
Web-based Graphical User Interface (GUI)	In this kind of user interface, user can use Microsoft Internet Explorer or other browser to control, guard and manage the device.
WINS Server	WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses. If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using the Windows Network Neighborhood feature.